

# Progetto S3/L5

Josh V. E. Abanico  
CS0525

13 dicembre 2025

## Indice

<b>1</b>	<b>Obiettivi del progetto</b>	<b>2</b>
1.1	Creazione policy con pfSense . . . . .	2
1.2	Schema della rete . . . . .	2
<b>2</b>	<b>Configurazione della rete</b>	<b>3</b>
2.1	Fase 1: Configurazione a macchine spente . . . . .	3
2.2	Fase 2: Configurazione Logica (pfSense) . . . . .	3
2.3	Fase 3: Servizi di Rete . . . . .	3
<b>3</b>	<b>Configurazione delle Regole del Firewall (pfSense)</b>	<b>5</b>
3.1	Accesso alla WebGUI . . . . .	5
3.2	Configurazione Interfacce e Regole . . . . .	5
3.2.1	1. Interfaccia WAN . . . . .	5
3.2.2	2. Interfaccia LAN (Rete Kali Linux) . . . . .	5
3.2.3	3. Interfaccia OPT1 (Rete Metasploitable) . . . . .	6
<b>4</b>	<b>Test e Verifica delle Configurazioni</b>	<b>8</b>
4.1	1. Test di Connettività (Ping) . . . . .	8
4.2	2. Test della Regola di Blocco (HTTP) . . . . .	9

# 1 Obiettivi del progetto

## 1.1 Creazione policy con pfSense

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a pfSense in modo tale da gestire una ulteriore rete.

## 1.2 Schema della rete

Analizzando bene la consegna, si può ottenere uno schema che vediamo nella *Figura 1*

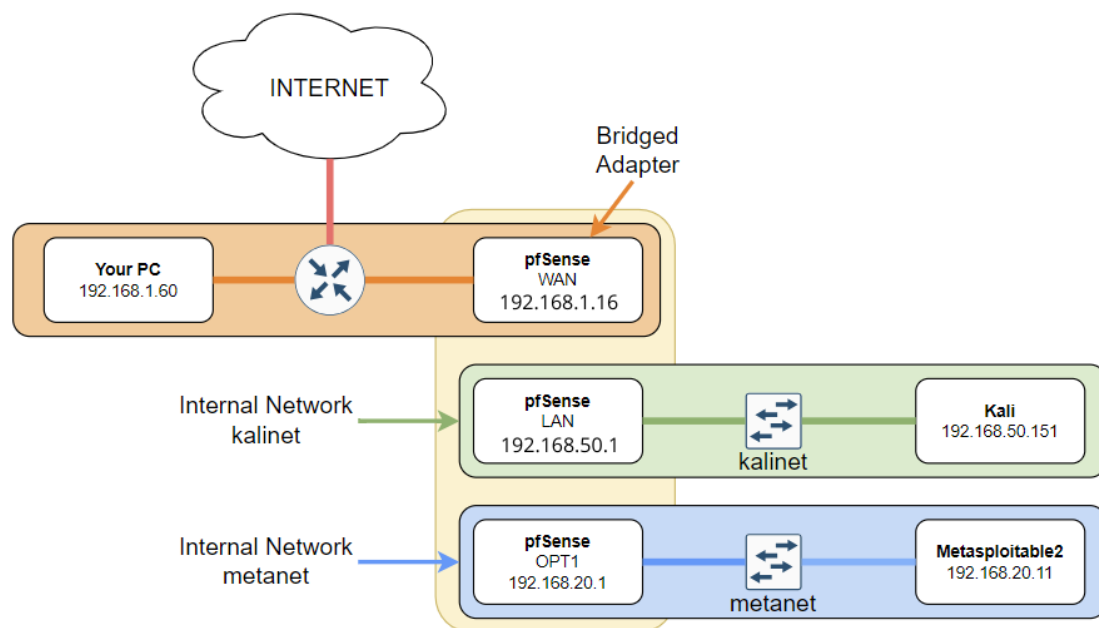


Figura 1: Schema della rete che realizzeremo

## 2 Configurazione della rete

### 2.1 Fase 1: Configurazione a macchine spente

Prima di avviare le macchine virtuali, è necessario configurare le interfacce di rete direttamente nelle impostazioni dell'hypervisor:

- **Kali Linux:** Impostare l'adattatore su Rete Interna (**kalinet**).
- **Metasploitable2:** Impostare l'adattatore su Rete Interna (**metanet**).
- **pfSense:** Configurare tre adattatori di rete distinti:
  1. **WAN (Bridge):** Connesso alla rete Wi-Fi/Fisica del PC ospitante.
  2. **LAN 1 (Rete Interna):** Connessa alla rete **kalinet**.
  3. **LAN 2 (Rete Interna):** Connessa alla rete **metanet**.

### 2.2 Fase 2: Configurazione Logica (pfSense)

Una volta accese le macchine, accediamo all'interfaccia di pfSense per configurare gli indirizzi IP e il routing tra le reti:

- **Interfaccia WAN:** IP statico 192.168.1.16 (oppure assegnato via DHCP dalla rete domestica).
- **Interfaccia LAN 1 (kalinet):** Impostare il Gateway su 192.168.50.1.
- **Interfaccia LAN 2 (metanet):** Impostare il Gateway su 192.168.20.1.

### 2.3 Fase 3: Servizi di Rete

- Abilitiamo il server **DHCP** su entrambe le interfacce interne (LAN 1 e LAN 2) del pfSense.
- Questo passaggio è fondamentale affinché Kali Linux e Metasploitable2 ricevano automaticamente un indirizzo IP all'avvio, evitando la configurazione manuale statica su ogni singola macchina.

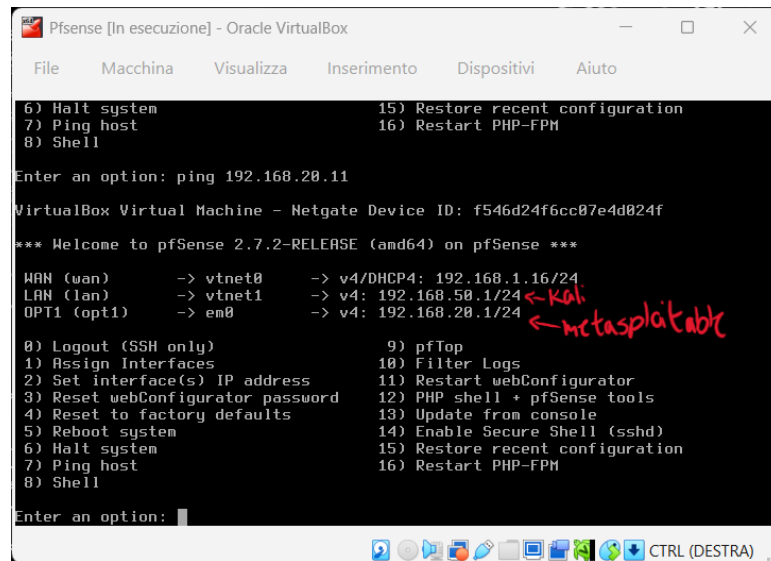


Figura 2: Configurazione pfSense

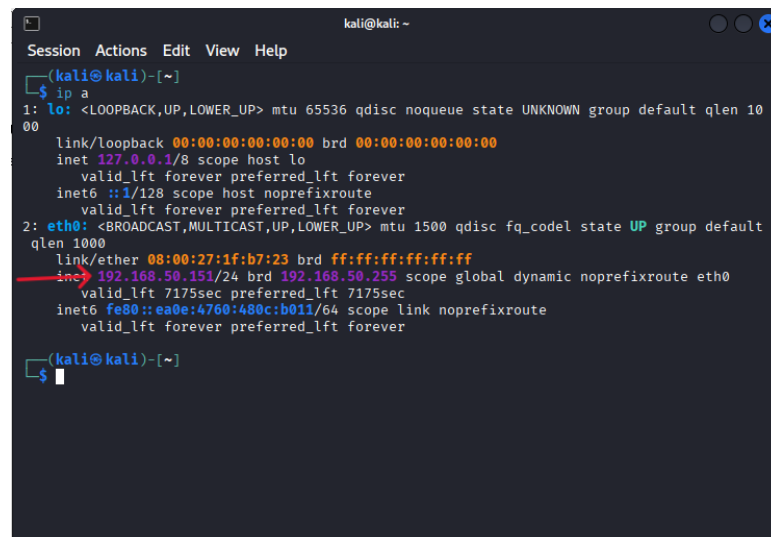


Figura 3: Indirizzo IP della macchina Kali

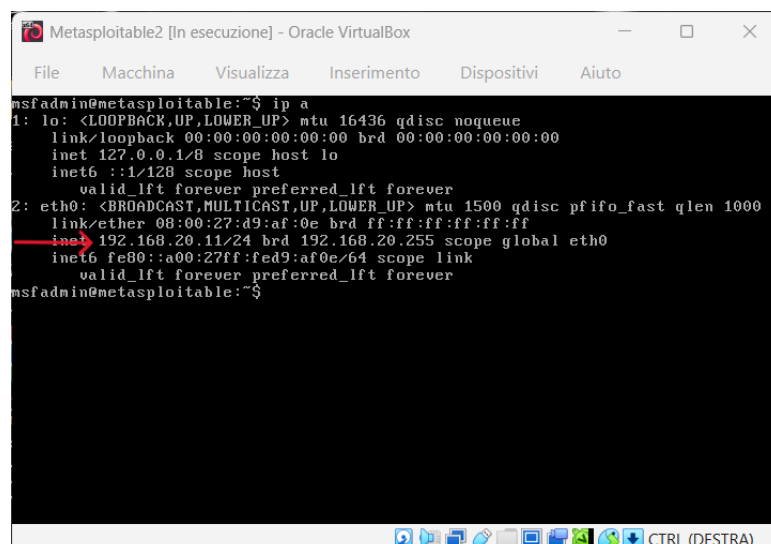


Figura 4: Indirizzo IP della macchina Metasploitable2

### 3 Configurazione delle Regole del Firewall (pfSense)

In questa fase definiremo le regole di filtraggio del traffico. Le configurazioni verranno applicate tramite l'interfaccia grafica (WebGUI) di pfSense.

#### 3.1 Accesso alla WebGUI

1. Avviare la macchina virtuale **Kali Linux**.
2. Aprire il browser (Firefox) e digitare nella barra degli indirizzi l'IP del gateway della rete **kalinet**: 192.168.50.1.
3. Effettuare il login con le credenziali di amministratore.

#### 3.2 Configurazione Interfacce e Regole

Navigare nel menu **Firewall** → **Rules**. Configureremo le regole per ciascuna interfaccia separatamente.

##### 3.2.1 1. Interfaccia WAN

- In questa sezione non apporteremo alcuna modifica. Lasciamo le configurazioni predefinite (che di norma bloccano il traffico in ingresso non richiesto).

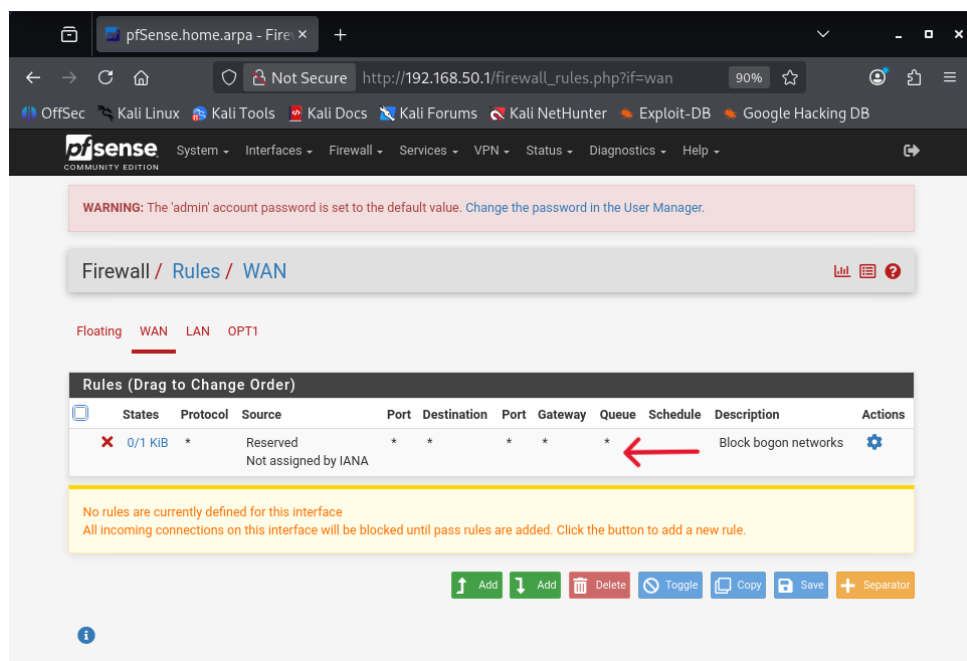


Figura 5: Regole della WAN

##### 3.2.2 2. Interfaccia LAN (Rete Kali Linux)

Qui imposteremo una regola per **bloccare** specificamente il traffico HTTP proveniente da Kali e diretto verso la Metasploitable2.

- Spostarsi sulla scheda **LAN**.
- Cliccare su **Add** (Aggiungi regola in alto).

- Configurare la regola come segue:
  - **Action:** Block (o Reject)
  - **Protocol:** TCP
  - **Source:** LAN net (o l'IP specifico della Kali)
  - **Destination:** Indirizzo IP della Metasploitable2 (rete metanet)
  - **Destination Port Range:** 80 (HTTP)
- **Risultato:** Questa regola impedirà qualsiasi connessione web verso la Metasploitable, rendendo irraggiungibile il servizio HTTP, pur mantenendo attivi gli altri servizi se non bloccati da altre regole.

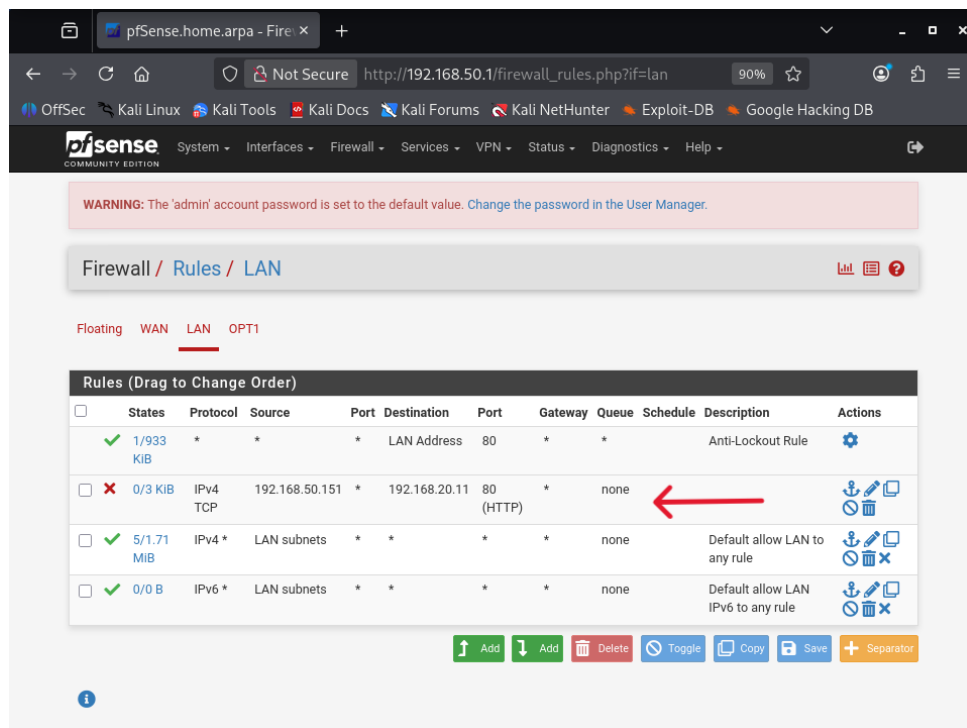


Figura 6: Regole della LAN

### 3.2.3 3. Interfaccia OPT1 (Rete Metasploitable)

Per la rete della macchina bersaglio (Metasploitable2), configureremo una regola permissiva per garantire che possa rispondere a qualsiasi richiesta e generare traffico in uscita senza restrizioni.

- Spostarsi sulla scheda **OPT1** (o il nome assegnato alla rete metanet).
- Aggiungere una regola di tipo "Pass Any":
  - **Action:** Pass
  - **Protocol:** Any
  - **Source:** OPT1 net
  - **Destination:** Any
- **Risultato:** Questo permette il passaggio di tutti i protocolli (ICMP, FTP, HTTP, HTTPS, ecc.) originati dalla rete Metasploitable, assicurando la piena connettività per i test.

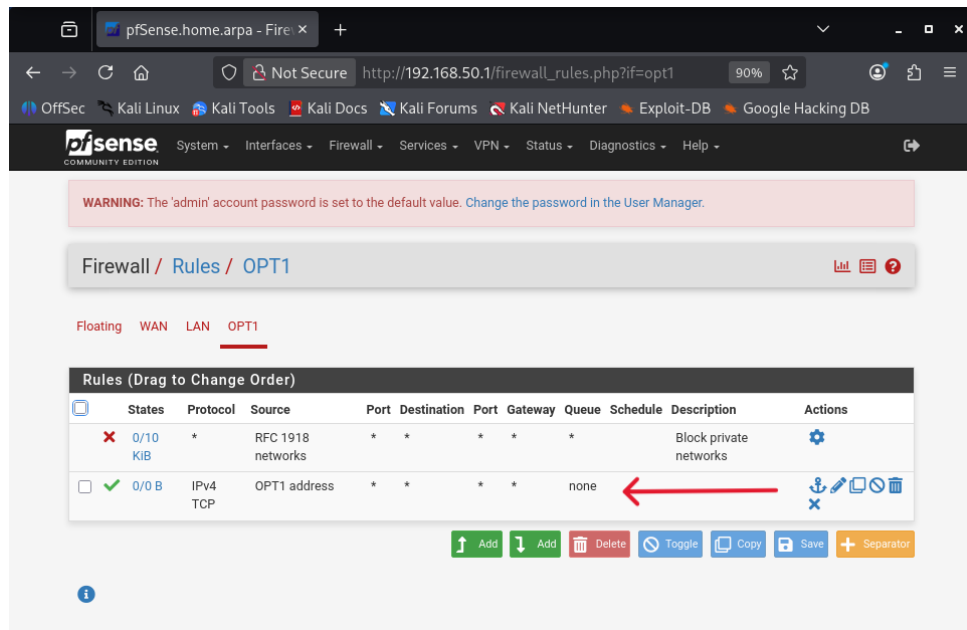


Figura 7: Regole della OPT1

**Nota Importante:** Ricordarsi sempre di cliccare sul pulsante **Apply Changes** dopo aver inserito le regole per renderle effettive.

## 4 Test e Verifica delle Configurazioni

L'ultimo passaggio consiste nel verificare che le regole imposte sul firewall funzionino come previsto: permettere la connettività di base (ICMP) ma bloccare specificamente il traffico Web (HTTP) proveniente da Kali.

### 4.1 1. Test di Connettività (Ping)

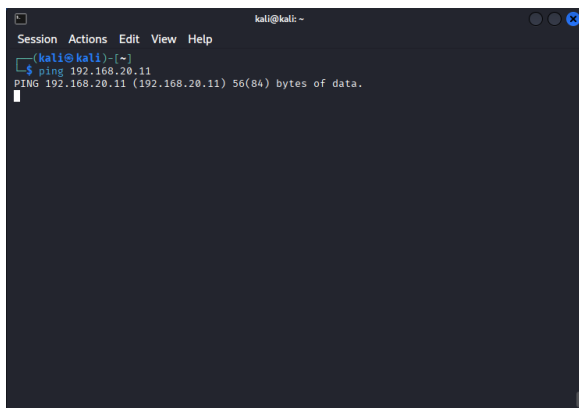
Verifichiamo innanzitutto che le due macchine riescano a comunicare a livello di rete.

- **Azione:** Dalla macchina **Kali Linux**, aprire il terminale ed eseguire il comando ping verso l'IP della Metasploitable2:

```
ping 192.168.20.11
```

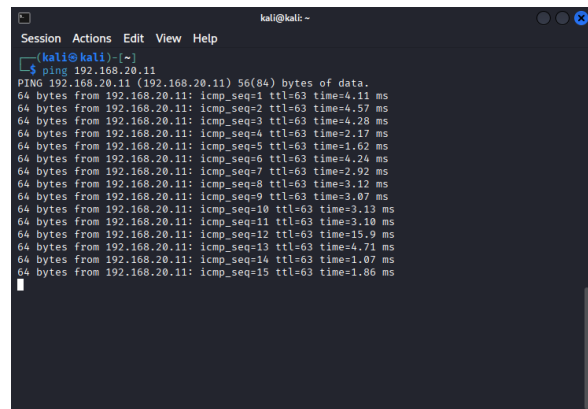
- **Osservazione:**

- *Prima della configurazione:* Il ping non andava a buon fine (spesso a causa della mancanza di regole di routing o di permesso sulla nuova interfaccia).
- *Stato attuale:* Ora il ping deve restituire una risposta positiva (64 bytes from...). Questo conferma che la regola **Pass Any** impostata sulla rete della Metasploitable (OPT1) permette correttamente il traffico di risposta.



```
kali@kali: ~  
$ ping 192.168.20.11  
PING 192.168.20.11 (192.168.20.11) 56(84) bytes of data.  
^
```

(a) Ping prima delle regole



```
kali@kali: ~  
$ ping 192.168.20.11  
PING 192.168.20.11 (192.168.20.11) 56(84) bytes of data.  
64 bytes from 192.168.20.11: icmp_seq=1 ttl=63 time=4.11 ms  
64 bytes from 192.168.20.11: icmp_seq=2 ttl=63 time=4.57 ms  
64 bytes from 192.168.20.11: icmp_seq=3 ttl=63 time=4.28 ms  
64 bytes from 192.168.20.11: icmp_seq=4 ttl=63 time=2.17 ms  
64 bytes from 192.168.20.11: icmp_seq=5 ttl=63 time=1.62 ms  
64 bytes from 192.168.20.11: icmp_seq=6 ttl=63 time=4.24 ms  
64 bytes from 192.168.20.11: icmp_seq=7 ttl=63 time=2.92 ms  
64 bytes from 192.168.20.11: icmp_seq=8 ttl=63 time=3.12 ms  
64 bytes from 192.168.20.11: icmp_seq=9 ttl=63 time=3.07 ms  
64 bytes from 192.168.20.11: icmp_seq=10 ttl=63 time=3.13 ms  
64 bytes from 192.168.20.11: icmp_seq=11 ttl=63 time=3.10 ms  
64 bytes from 192.168.20.11: icmp_seq=12 ttl=63 time=15.9 ms  
64 bytes from 192.168.20.11: icmp_seq=13 ttl=63 time=4.71 ms  
64 bytes from 192.168.20.11: icmp_seq=14 ttl=63 time=1.07 ms  
64 bytes from 192.168.20.11: icmp_seq=15 ttl=63 time=1.86 ms  
^
```

(b) Ping dopo le regole

## 4.2 2. Test della Regola di Blocco (HTTP)

Ora verifichiamo l'efficacia della regola di sicurezza che blocca la porta 80.

- **Azione:** Aprire il browser web su **Kali Linux** e tentare di accedere all'interfaccia web della Metasploitable digitando nella barra degli indirizzi:

`http://192.168.20.11`

- **Osservazione:**

- *Prima della regola:* L'accesso alla pagina web avveniva correttamente, mostrando la home page di Metasploitable2.

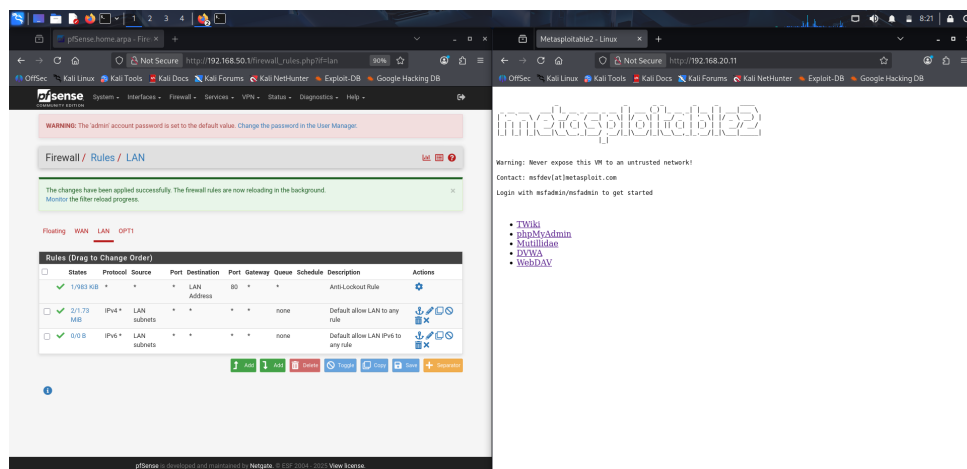


Figura 9: Sito Metasploitable2 prima le regole

- *Stato attuale:* Il browser non riesce a caricare la pagina (errore di *Connection Timed Out* o *Connection Refused*).

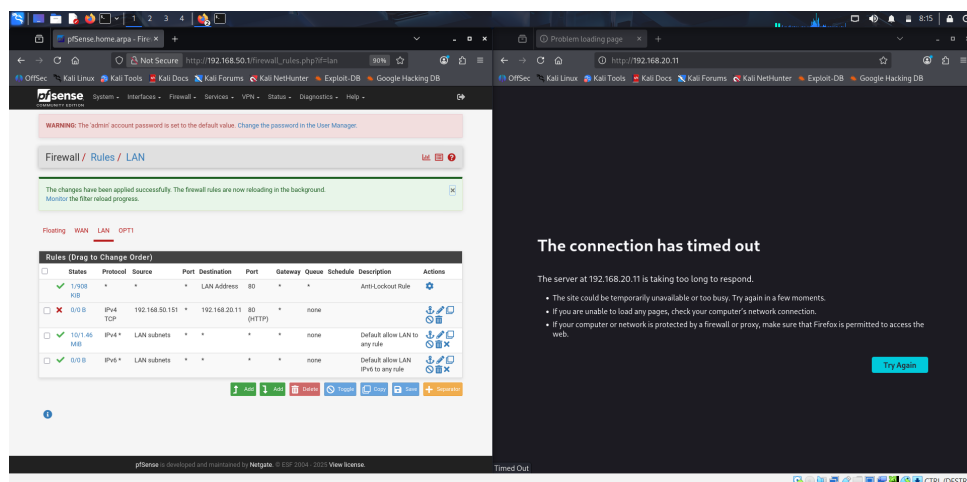


Figura 10: Sito Metasploitable2 dopo le regole

- **Conclusione:** Il test ha successo. Il firewall pfSense sta correttamente bloccando i pacchetti TCP sulla porta 80, mentre lascia passare gli altri tipi di traffico (come dimostrato dal Ping funzionante).